EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

May 1, 2021 - Volume 13, Issue 8

Statement from U.S. Secretary of Commerce Gina M. Raimondo on Q1 2021 GDP Advance Estimate

FOR IMMEDIATE RELEASE
April 29, 2021

Media Contact: PublicAffairs@doc.gov

Statement from U.S. Secretary of Commerce Gina M. Raimondo on Q1 2021 GDP Advance Estimate

WASHINGTON -- Today, the Department of Commerce's Bureau of Economic Analysis (BEA) released the advance estimate for gross domestic product (GDP) for the first quarter of 2021, finding that real gross domestic product increased at a 6.4-percent annual rate. Personal consumption expenditures increased by a robust 10.7-percent annual rate, while business investment in equipment and intellectual property products continued to grow steadily.

NEWSLETTER NOTES

SAP RESOLVES ALLEGATIONS OF EXPORT CONTROL LAW VIOLATIONS WITH $3.29 MILLION ADMINISTRATIVE SETTLEMENT

FOR IMMEDIATE RELEASE BUREAU OF INDUSTRY AND SECURITY

April 29, 2021
Office of Congressional and Public Affairs
www.bis.doc.gov (202) 482-1069

On April 29 2021, Kevin J. Kurland, Acting Assistant Secretary for Export Enforcement, Bureau of Industry and Security (BIS) of the U.S. Department of Commerce, announced an administrative settlement of $3,290,000 with SAP SE (SAP), a multinational software company based in Walldorf, Germany. SAP also agreed to complete three audits of its export compliance program over a three year period. SAP voluntarily self-disclosed potential violations of the Export Administration Regulations (EAR) to BIS, and cooperated with the investigation conducted by the Boston Field Office of BIS's Office of Export Enforcement.

"The Bureau of Industry and Security strongly encourages companies, including software providers, to maintain robust export compliance programs to prevent violations of the EAR," said Mr. Kurland. "If violations do occur, submitting a voluntary self-disclosure of the violations to BIS will be a significant mitigating factor in any penalties imposed."

This settlement resolves BIS's allegations that, during a period including December 2009 through September 2019, SAP engaged in conduct prohibited by the EAR when it exported SAP products including software, upgrades, and patches from the United States to various end users located in sanctioned countries, including Iran, without the required export licenses. The items were controlled for encryption and national security reasons. The U.S. Department of Justice and Office of Foreign Assets Control of the U.S. Department of the Treasury also entered into agreed-upon resolutions with SAP involving related conduct of concern.

BIS's mission is to advance U.S. national security and foreign policy objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. Among its enforcement efforts, BIS is committed to preventing U.S.-origin items from supporting Weapons of Mass Destruction projects, terrorist activities, or destabilizing military modernization programs. For more information, please visit www.bis.doc.gov .

Settlement Agreements between the U.S. Department of the Treasury's Office of Foreign Assets Control and MoneyGram Payment Systems, Inc., and SAP SE

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) today announced a settlement with MoneyGram Payment Systems, Inc. ("MoneyGram"), a global payments company based in Dallas, Texas that allows people to send money in more than 200 countries and territories. MoneyGram agreed to remit $34,328.78 to settle its potential civil liability for 359 apparent violations of multiple sanctions programs. MoneyGram provided services to blocked individuals incarcerated in U.S. federal prisons without a license from OFAC, processed transactions on behalf of an additional blocked person, and processed transactions for individuals who initiated commercial transactions involving Syria.

For more information regarding today's settlement with MoneyGram, please visit the following web notice.

Separately, OFAC has announced a $2,132,174 settlement with SAP SE ("SAP"). SAP, a software company located in Walldorf, Germany has agreed to settle its potential civil liability for 190 apparent violations of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560. Specifically, between approximately 2013 and 2018, SAP engaged in the export, re-export, sale, or supply of technology or services from the United States to companies in third countries with knowledge or reason to know the software or services were intended specifically for Iran, and sold cloud-based software subscription services accessed remotely through SAP's cloud businesses in the United States to customers that made the services available to their employees in Iran. OFAC determined that SAP voluntarily self-disclosed the apparent violations, and that these apparent violations constitute a non-egregious case. For more information regarding today's settlement with SAP, please visit the following web notice.

For more information on this specific action, please visit this page.

Raúl Castro says he is resigning as Cuban Communist Party leader, ending his family's six decades in power.

Mr Castro, 89, told a party congress that he is handing over the leadership to a younger generation "full of passion and anti-imperialist spirit".

His successor will be voted in at the end of the four-day congress.

The move, which was expected, ends the era of formal leadership by him and his brother Fidel Castro, which began with the 1959 revolution.

"I believe fervently in the strength and exemplary nature and comprehension of my compatriots," he told party delegates in Havana on Friday.

Although Mr Castro has not endorsed a successor, it is widely believed the party leadership will pass to Miguel Díaz-Canel, who took over as the island's president in 2018.

FOR IMMEDIATE RELEASE BUREAU OF INDUSTRY AND SECURITY

G. Nagesh Rao Appointed to Chief Information Officer The Bureau of Industry and Security (BIS) within the US Department of Commerce is pleased to announce the appointment of G. Nagesh Rao as Chief Information Officer, and his selection to the career Senior Executive Service ranks. Mr. Rao, an Eisenhower Fellow and a Mirzayan Science and Technology Policy Fellow, brings a wealth of experience to BIS having worked in the Public, Private, and NGO sectors over the last 20+ years, where he has had extensive experience working on IP-Portfolios, Global Strategies, Consumer Products, and Technology R&D, for a variety of leading companies in the private sector. He holds degrees from Rensselaer Polytechnic Institute, Albany Law School, and University of Maryland-College Park. Prior to coming to BIS, he worked at the U.S. Small Business Administration (SBA) and served on the COVID-19 Leadership Response Team, supporting the historic CARES Act implementation and overseeing build out and modernization of key digital products including PPP Lender Gateway, SBIR.Gov, and SBA.Gov. In the past 10 months while at BIS, Mr. Rao oversaw the first wave of technology modernization efforts which included cloud adoption, remote-work capabilities, and software as a service (SaaS) based solutions helping bring the bureau up to speed on a current technology stack standard, which in part earned him a FCW 2021 Fed 100 award.

Wyden Releases Draft Legislation to Protect Americans' Personal Data From Hostile Foreign Governments

Washington, D.C. – U.S. Senator Ron Wyden, D-Ore., released a discussion draft of legislation to regulate the export of Americans' sensitive personal information to potentially hostile foreign nations.

The Protecting Americans' Data from Foreign Surveillance Act would create new safeguards against exporting sensitive personal information to foreign countries if doing so could harm U.S. national security.

"Shady data brokers shouldn't get rich selling Americans' private data to foreign countries that could use it to threaten our national security," Wyden said. "My bill would set up common sense rules for how and where sensitive data can be shared overseas, to make sure that foreign criminals and spies don't get their hands on it. This legislation is another piece in a slate of bills I'm introducing this Congress to provide comprehensive protection for Americans' sensitive information."

Director of National Intelligence Avril Haines testified on Wednesday that the transfer of personal information to foreign adversaries represents a security threat:

"I agree with you that there's a concern about foreign adversaries getting commercially-acquired information as well and am absolutely committed to trying to do everything we can to reduce that possibility," she said, in response to a question from Wyden.

This bill builds on the 2018 Foreign Investment Risk Review Modernization Act, in which Congress directed CFIUS to review and if necessary, stop the purchase of U.S. firms holding large amounts of Americans' personal data, and an executive order from earlier this year requiring recommendations to restrict the transfer of data to foreign adversaries.

Read the full bill here. Wyden is seeking comments on the proposal at ExportControl_Feedback@wyden.senate.gov.

*(*Continued On The Following Page)*

The draft legislation:

- Directs the Secretary of Commerce to lead an interagency process to identify categories of personal data that, if exported by third parties, could harm U.S. national security.

- Directs the Secretary of Commerce to compile a list of countries to which exports of Americans' personal data would not harm national security, and to require licenses for exports of the identified categories of personal data to other countries in bulk, based on:Exempts from the new export controls any data encrypted with NIST-approved algorithms, if the key protecting the data is not exported.
- the adequacy and enforcement of data protection, surveillance, and export control laws in the foreign country.
- the circumstances under which the government of the foreign country can compel, coerce, or pay a person in that country to disclose personal data.
- whether that government has conducted hostile foreign intelligence operations against the United States.

- Ensures that the export rules do not apply to journalism and other speech protected by the First Amendment.

- Applies export control penalties to senior executives who knew or should have known that employees below them were directed to illegally export Americans' personal data.

- Creates a private right of action for individuals who have been physically harmed or arrested or detained in a foreign country as a result of the illegal export of personal data.

- Requires the Commerce Department to publish quarterly reports on personal data exports.

Wyden is the leading Congressional advocate for securing Americans' private information, against threats from hackers and foreign governments, as well as protecting Americans' rights against unnecessary government surveillance. He introduced the Mind Your Own Business Act last year, to provide strong new protections against unauthorized sharing Americans data for commercial reasons

Secretary Raimondo Joins Vice President Harris in Addressing Care Economy and Need to Invest in Human Infrastructure

April 19, 2021

Earlier this month, U.S. Secretary of Commerce Gina Raimondo joined Vice President Kamala Harris, Speaker of the House Nancy Pelosi, and other leaders and stakeholders in addressing the first-ever Care Can't Wait Summit. The summit convened caregivers, care workers, people with disabilities, older adults, children, parents & grandparents, advocates & policy leaders virtually across the United States to build a stronger, broader base of support for public investment in the care infrastructure as part of the Biden Administration's American Jobs Plan.

Today there are 53 million unpaid family caregivers in the United States. At the beginning of the pandemic, the childcare sector lost 400,000 jobs and many are still unemployed. American families continue to struggle as women, most notably women of color, have been forced out of the workforce. Through the American Jobs Plan, the Biden Administration is working to provide the critical infrastructure needed to support our Nation's caregivers so they can earn a living and care for their loved ones.

Secretary Raimondo was among one of the first speakers at the summit and addressed the importance of our Nation's caregivers to our economic recovery and investing in a strong care infrastructure.

"The pandemic has shown us the importance of care work. Care is infrastructure," said Secretary Raimondo. "We must create the infrastructure and provide the resources to take care of our caregivers."

Secretary Raimondo also stressed that the care economy is core to American competitiveness and that it is not only a business issue, but an "everybody issue." She shared that this issue is near and dear to her heart and that she is thankful she has had support for the past 15 years in raising her children and having a care team today that allows her 90-year old mother to age with dignity.

"There are millions of women, mostly women of color, unbelievably hardworking, working full time in poverty, taking care of our loved ones," she said. "That's WRONG. It's time to build the infrastructure required so people aren't living in poverty."

*(*Continued On The Following Page)*

During the summit, Speaker of the House Nancy Pelosi stressed, “Investing in the care economy is a necessity and it’s a matter of justice.”

Later in the day, Vice President Kamala Harris joined the summit and outlined the Biden Administration’s American Jobs Plan and how it will include the care economy.

“We are expanding the definition of infrastructure, it’s not only about roads and bridges and water and broadband; it’s about care,” said Vice President Harris. “The American Jobs Plan invests $400 billion into our country’s infrastructure, our human infrastructure.”

The American Jobs Plan proposes substantial investments in the infrastructure of our care economy and creating new and better jobs for caregiving workers. Vice President Harris announced that in the coming weeks, the Administration will build on the American Jobs Plan with the American Family Plan.

“We want to create an economy where care is readily available for those who need it,” she said. “We want to ensure caregivers are treated with respect. In supporting this economy, we will create the kind of change that lasts for generations. For caregivers, that means better wages, more protections, and more security. For families that means more accessibility and more affordability.”

The Care Can’t Wait Summit was hosted by Ai-jen Poo, director of Caring Across Generations, a national group advocating for the care of older adults, individuals with disabilities, families and caregivers.

SpaceX launches crew of four on way to space station

The flight is the third with astronauts on board for SpaceX in the past year and the first where NASA allowed SpaceX to reuse equipment from previous flights. On board are two American astronauts, one from France and one from Japan. They are scheduled to spend six months at the International Space Station, where they’ll arrive early Saturday.

Whether You Build Them or Buy Them – IoT Device Security Concerns Us All

April 15, 2021

The Internet of Things (IoT) offers many attractions for small and medium-sized manufacturers (SMMs) who may want to integrate IoT into their facilities and operations, or who seek to enter the IoT market with innovative products. The spectrum of available IoT products is broad and continually growing. When venturing into the IoT waters, it’s helpful to be prepared for the potential cybersecurity pitfalls, whether in the form of implications for organizational risk management when introducing IoT to the environment or considerations for product design and support when entering the marketplace as a product vendor. The NIST Cybersecurity for the Internet of Things program is working to provide the information that SMMs need to navigate these potentially turbulent waters.

IoT and Risk Management

Before you install smart thermostats to keep your employees comfortable, add smart coffee pots to break rooms to keep them caffeinated or deploy the latest and greatest Industrial Control System (ICS) technology in your production environment, it’s important to recognize the potential implications. You may have a robust information security program for your traditional IT, but those tools, processes and procedures will likely require adaptation when IoT is introduced. Some of the ways that IoT is different include:

- Interacting with the physical world. IoT devices are equipped either with sensors that collect information from their environment or actuators that cause “real world” objects to move or change. Sensing can generate a lot of potentially sensitive data, so knowing what is collected and where it’s going is important. A compromised actuator could enable an adversary to cause significant disruption – think what could happen if you don’t know who is commanding your smart locks.
- Challenging conventional IT management practices. IoT devices are often “black boxes” that both obscure their internal goings-on and can’t be equipped with agents or queried in the same manner as servers, desktops or firewalls. As a result, common IT management practices can prove ineffective with IoT. These management challenges can multiply quickly if you’re deploying IoT devices “at scale.”

*(*Continued On The Following Page)*

Lacking common cybersecurity and privacy features. IoT devices often lack support for logging and monitoring, support for updating devices to address newly identified vulnerabilities, or cryptographic capabilities needed to protect sensitive information they generate or process. It cannot be assumed these devices possess the same cybersecurity capabilities as IT devices on the same network.
SMMs adopting IoT into their environments need to be prepared to address these challenges. If entering the IoT market as a vendor, understanding these challenges can be an opportunity to develop a product that provides a better customer experience.

Managing Your IoT Security Risk

When adopting IoT technology in your organization, SMMs should plan to address these challenges with an eye toward three goals:

- Protecting IoT device security to ensure that the product is fully under the owner's control, and not being exploited by outside actors to gain access to the SMM's network or participate in a botnet.
- Protecting data security so that data generated by IoT devices isn't exposed or altered while stored on the devices, transferred across the network or transmitted to a cloud-based service used to provide aspects of the product's capabilities.
- Protecting individuals' privacy, being alert to the possibility of privacy-sensitive information being captured or created by IoT products, and cognizant of where that data might travel.

These goals are articulated in NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, and can be difficult to achieve with currently available IoT products. For organizations that are applying the NIST Cybersecurity Framework (CSF) or defining their security requirements using NIST SP 800-53 controls, NISTIR 8228 identifies a range of challenges that IoT devices present to achieving the ends that the CSF and SP 800-53 intend. For example, control SI-2, Flaw Remediation, from SP 800-53 cannot be satisfied by IoT devices that lack an ability for secure software/firmware updates. Similarly, many IoT devices cannot be analyzed in a manner needed to satisfy the CSF subcategory DE.CM-8: Vulnerability scans that are performed.

Consideration for the three goals identified above should factor into the selection of IoT products as well as how they are managed, as the security capabilities of IoT devices contribute to achieving the overall security requirements of the systems into which the devices are integrated.

*(*Continued On The Following Column)*

Improving Your IoT Products' Security Posture

If you are venturing into the creation of IoT products, awareness of cybersecurity challenges can help guide your approach to the development and support of your product. The three goals described above also apply when developing an IoT product. A thoughtful approach to development with those goals in mind will result in a more manageable, more secure product. This approach involves both the design and development phase for the product and the support phase once it's brought to market, as illustrated in this figure from NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers.

The core baselines outline device abilities and supporting actions across a spectrum of needs:

Technical Cybersecurity Capabilities

Device Identification: The IoT device can be uniquely identified logically and physically.

Device Configuration: The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.

Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.

Logical Access to Interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.

Software Update: The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.

Cybersecurity State Awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.

Non-Technical Supporting Capabilities

Documentation: The ability for the manufacturer and/or supporting entity to create, gather and store information relevant to cybersecurity of the IoT device throughout the development of a device and its subsequent lifecycle.

Information and Query Reception: The ability for the manufacturer and/or supporting entity to receive from the customer information and queries related to cybersecurity of the IoT device.

(*Continued On The Following Page)

Information Dissemination: The ability for the manufacturer and/or supporting entity to broadcast and distribute information related to cybersecurity of the IoT device.

Education and Awareness: The ability for the manufacturer and/or supporting entity to create awareness of and educate customers about elements such as cybersecurity-related information, considerations and features of the IoT device. The planning activities combined with applying the technical and non-technical baselines will help SMMs develop products that are both more secure-able and better supported, helping your customers to take advantage of your IoT innovations while limiting the impact to their risk management challenges.

Information That Can Help

The NIST Cybersecurity for the Internet of Things program has engaged deeply with the community over the last several years and developed a rich collection of guidance around IoT cybersecurity challenges. Whether you are an SMM looking to improve operations with the integration of IoT or enter the marketplace with new products, there are many resources and publications available to assist your efforts.

NIST's Cybersecurity for IoT welcomes manufacturer feedback

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)

"You've got to get up every morning with determination if you're going to go to bed with satisfaction." —George Lorimer

Commerce Secretary Gina M. Raimondo to Head U.S. Delegation at G7 Digital & Technology Ministerial

FOR IMMEDIATE RELEASE
April 27, 2021
Media Contact: PublicAffairs@doc.gov

WASHINGTON – U.S. Secretary of Commerce Gina M. Raimondo will lead the United States' virtual delegation at the Group of Seven (G7) Digital and Technology Ministerial on April 28 through April 29. The meeting will underscore the necessity of connectivity and digital technologies in facilitating the collaboration among countries necessary to tackle the COVID-19 pandemic and other shared challenges. Secretary Raimondo will speak to the United States' goals of securing the free flow of data with trust, strengthening an open and industry-led global standards system, and fostering 5G vendor diversity, as well as reaffirming the United States' commitment to advancing technology leadership domestically and internationally.

"It is my honor to represent the U.S. government at this week's G7 Ministerial meeting," said Secretary Raimondo. "The G7 Digital and Technology Ministerial meeting is a unique opportunity to underscore the critical importance of the digital economy to not just the G7 countries but for the world. The shared values and commitments among G7 members will play an essential role in supporting a vibrant tech sector that continues to innovate and develop solutions and technologies that advance the well-being of all people." Jason Matheny, Deputy Assistant to the President for Technology and National Security, will join Secretary Raimondo as part of the U.S. delegation to the Ministerial. The meeting will be held virtually and hosted by the United Kingdom as part of their G7 Presidency.